

# مجلة كلية التراث الجامعة

مجلة علمية محكمة  
متعددة التخصصات نصف سنوية  
العدد الأربعون

30 آب 2024  
ISSN 2074-5621



رئيس هيئة التحرير

أ.د. جعفر جابر جواد

مدير التحرير

أ.م. د. حيدر محمود سلمان

رقم الايداع في دار الكتب والوثائق 719 لسنة 2011

مجلة كلية التراث الجامعة معترف بها من قبل وزارة التعليم العالي والبحث العلمي بكتابها المرقم  
(ب 3059/4) والمؤرخ في (2014/ 4/7)

## Using Steganography, Cryptography and QR Code to Secure Data

Shahbaa Mohammed Abdulmaged<sup>1\*</sup>

Nadia Mohammed Abdulmaged<sup>2</sup>

<sup>1</sup>Law Dep. College of Law and Political Science, Al-Iraqia University  
Baghdad/ Iraq

<sup>2</sup>Computer Dep. College of Education for Pure Science  
/Ibn-Alhaitham, Baghdad University  
Baghdad/ Iraq

\* Corresponding author: Shahbaa Mohammed Abdulmaged, email: narimanfn@gmail.com

Safeguarding information can be said to be one of the significant features of today's computing systems. Significantly higher protection standards must be employed to protect sensitive information from unauthorized access because of the increasing risk of cyberscheme attacks. The years have seen many people presenting different ideas to incorporate other forms of security measures for instance steganography, cryptography and color QR code technology. Integrating these techniques help protect the data from cyber-criminal as well as other forms of attacks.

In this research paper, the ideas of steganography, cryptography and color QR code technology will be discussed to outline the ways to improve data security. In this paper will show how these technique can be used in combination to ensure a sound security solution that covers confidentiality, integrity and availability. Also, an overview of certain features of each method and how they can employed in synergy will be discussed deeper.

The techniques mentioned here will also discussed in this paper concerning the difficulties facing their execution and possible approaches to them. Lastly, it is the goal of this research paper to give the reader an understanding on how the integration of steganography, cryptography and color QR code technology can improve data protection mechanisms.

**Keywords:** data security, steganography, cryptography, color QR code, LSB.

### Introduction

Security of data is the most crucial matter in the modern world surrounded by technologies. The combination of steganography, cryptography and color QR code technology that is proposed here forms a robust data security regime with high entropy as well as a high degree of data hiding capability [1]. An approach offers a good way of securing data confidentiality and integrity of the data against many threats [1]. When steganography is combined with cryptography, there is a greater protection to data by hiding them in digital media [2]. Cryptography and steganography when implement in conjunction offer considerably more security to data than if either method was used alone [2]. These technologies have universal applicability in different domains including

mobile devices, system login authentication, and cloud computing implying the significant significance of the technologies in the protection of organizational information integrity and confidentiality in contemporary society [2, 3].

There are a number of principles that would define the effective data security strategy and it can be concluded that using a diversified approach to the problem is the only right solution. This implies establishing coherence between steganography, cryptography and color QR code. Steganography is a process of hiding data in other less suspicious data; cryptography serves to optimize the encryption process and at the same time the use of color QR code makes it quite efficient and secure means of transferring secure data. Combined, these techniques constitute a tough barrier that protects data that needs to be protected in a hyperconnected world.

### **Background and related work**

#### **How does color QR code technology strengthen data security measures?**

Color QR code technology can also be used for steganography when transferred remotely, to transfer sensitive data [4]. Here, it is made possible to store specific and voluminous information within an image that can be transmitted inconspicuously. Thus, the security of data as far as the users is well enhanced since the intruders will not be able to understand the encrypted data.

By adding some different color within the QR code, message can be embed within the code itself [5]. New opportunity for hiding text message has been provided by utilizing color QR code to hide text has given a new approach. However, where the previous technique might have fallen short, is in the integration of text into the code; for example, if a gradient or pattern is used within the QR code, text can be incorporated into the code with barely any effect on scanning capability. In addition, prior studies establish that color-coded QR code also exhibit a higher decoding rate than black and white QR code.

In conclusion, the color QR code technology has a great potential in creating secured data management platform through the courses of adopting top class encryption process along with steganography.

### **Related work**

The paper [6] presented a new steganography and QR code-based data security approach. Any QR code reader may readily decrypt a message contained within a QR code. However, the secret and security are improved because the suggested method uses steganography.

This paper [7] using cryptography, by XORing the secret message with a QR code, the encrypted message was recovered. The encrypted message was concealed in locations chosen by the bat algorithm while employing the LSB (Least Significant Bit) technique for steganography, and the utilization of the QR technique at the end revealed enhanced security and integrity based on the parameters.

In [8] paper uses QR Code images as secret codes, transforming them into an array of bits and inserting them into the blue channel in dual carrier images. The model's performance was

evaluated using MSE (mean squared error), PSNR (peak signal to noise ratio), Hiding Capacity, Histogram, recovery, and noise tests, showing high PSNR values and a 100% recovery rate.

### **Proposed Approach**

A color QR code generator converts the secret text into color QR code that are unintelligible to humans and encrypts the content. However, any smartphone with a built in camera can readily interpret the content concealed in these color QR code. A novel approach that combines color QR code with cryptography and steganography techniques is proposed in order to maintain the text's confidentiality and prevent unwanted access.

The suggested approach includes methods for hiding, ciphering, and encoding at the transmitter and the opposite procedures at the recipient.

### **Transmitting procedure**

The encoding procedure entails first encrypting the secret text into color QR code and then embedding color QR code into a colored image (cover image). The actions that make up this procedure are:

1. Choose the secret text and cipher it.
2. Use any color QR code generator to create a color QR code out of it. ([9] <https://www.qrcode-tiger.com>) and hide the cipher text in it.
3. Utilizing the LSB replacement approach, read a cover image and embed the color QR code's quantized bits into the image's pixels..
4. Save the stego image.

A steganography method needs to provide assurance of visual imperceptibility. This is achieved by quantizing the color QR code, which is then embedded into the color image to reduce the number of changes in the color image's luminance. A color pattern matrix makes up a color QR code. By converting these patterns into binary streams of 0 and 1, the suggested approach significantly lowers the number of bits that need to be embedded. Therefore, there will not be any noticeable distortion that the unaided eye can see when a color QR code is embedded in a cover image.

### **Receiving procedure**

The decoding procedure entails extracting the color QR code from the stego image and extracting the cipher text from it and deciphering it. The actions that make up this procedure are:

1. Read the stego image.
2. From the stego image, extract the quantized bits of the color QR code.
3. Bits are dequantized to create colored QR code.
4. Scan the color QR code that contains the hidden text with any kind of QR code reader (smartphone camera) and decipher it.

Multiple color QR code containing varied sized texts have been used to test the suggested approach.

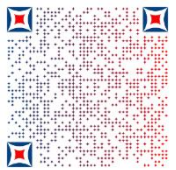


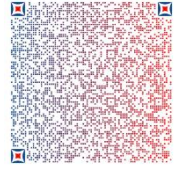


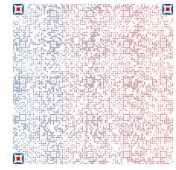


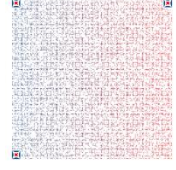


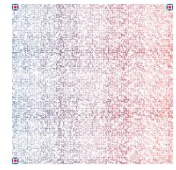


The original concealed text and the retrieved text are identical. The following section discusses the test findings.

## **RESULTS AND ANALYSIS**

### **Results**

The execution is done with the Windows 10 operating system in Matlab (R2022b) software. Table 1 displays the outcome of testing this approach using example secret texts ranging in size from 60 to 1146 bytes. The color QR column illustrates how the amount of the encrypted text affects the pattern and intricacy of the color QR code. When massive amounts of data are encrypted, the color QR pattern's complexity will rise.

Table 1: outcome of encoding procedure.

Size of the secret text	Color QR code (200×200)	Cover image (512 × 512)	Stego image (512 × 512)
60 bytes			
238 bytes			
409 bytes			
693 bytes			
1.11 KB			

### Analysis

Imperceptibility is the most critical requirement that any data embedding approach must satisfy. It is measured by mean square error (MSE) and peak signal to noise ratio (PSNR) values, where a high PSNR implies a high level of imperceptibility [10].

### Mean Square Error (MSE)

The MSE is the mean squared error value between the original image (cover image) and the image of the insertion (stego image) as shown in (1):

$$MSE = \frac{1}{(N \times M)^2} \sum_{i=1}^N \sum_{j=1}^M (X_{ij} - Y_{ij})^2 \quad (1)$$

Where

M= the No. of lines on the cover image

N= the No. of columns on the cover image

$X_{ij}$ = the intensity of the cover image

$Y_{ij}$ = the intensity of the stego image

#### Peak Signal to Noise Ratio (PSNR)

The PSNR in decibels is computed between the cover image and the stego image. PSNR can be defined as in (2):

$$PSNR = 10 \log_{10} \left[ \frac{I^2}{MSE} \right] \quad (2)$$

Where

MSE Mean Square Error value obtained

$I^2$ = the maximum value of the image pixels used.

Several images were used with texts of different sizes, PSNR and MSE were calculated for each of them, as explained in the table II.

Table 2: PSNR and MSE.

Image name	Peppers	Leaf&palm	Building	Leaf	Sand
Image size	512 × 512	512 × 512	512 × 512	512 × 512	512 × 512
Text size	60 bytes	238 bytes	409 bytes	693 bytes	1.26 KB
MSE	0.01486	0.01597	0.01608	0.01719	0.01820
Highest PSNR of stego image	89.8769	87.6436	85.4103	83.2970	81.0649

Table 3 shows a complete comparison between related work and the proposed approach, from the results, we note that the proposed approach has achieved higher results than the others have.

Table 3: comparison between related work & proposed approach.

Approaches	Image size	Hiding capacity	PSNR	MSE
[6]	512 × 512	12.5%	52.585	0.601
[7]	512 × 512	12.5%	81.6013	0.9897
[8]	512 × 512	12.5%	64.7850	0.0216
Proposed	512 × 512	12.5%	87.6436	0.01597

#### Conclusion

In the dynamic field of data security, a novel approach emerges — the fusion of cryptography, steganography, and color QR Code. This research article delves into the seamless integration of these three elements, offering a robust solution for secure communication.



The integration of steganography, cryptography, and color QR code technology has proven to be a promising approach to enhancing data security measures. Steganography provides an additional layer of security by hiding data within an image, making it difficult for unauthorized users to detect the presence of sensitive information. Moreover, using steganography in combination with cryptography further strengthens data security measures, making it almost impossible for hackers to access confidential data.

The innovative approach of color QR code technology, which uses advanced encryption techniques and steganography, has further enhanced data security measures. However, despite the numerous benefits of this approach, there are potential limitations and biases that need to be addressed to ensure its effectiveness. Future research should focus on addressing these limitations and biases to further improve data security measures and advance knowledge in this field.

### References

- [1] N. A. Mawla, H. K. Khafaji, "Enhancing Data Security: A Cutting-Edge Approach Utilizing Protein Chains in Cryptography and Steganography", *Computers*, Vol.12, 8: 166, 2023. <https://doi.org/10.3390/computers12080166>
- [2] A. Jan, S. A. Parah, M. Hussan, et al, "Double layer security using crypto-stego techniques: a comprehensive review", *Health Technol*, 12, 9–31. 2022. <https://doi.org/10.1007/s12553-021-00602-1>
- [3] S. M. Abdulmaged, N. M. Abdulmaged, "A new steganography technique based on genetic algorithm", *Global Journal of Engineering and Technology Advances*, vol.16, 2, 135–139, 2023. <https://doi.org/10.30574/gjeta.2023.16.2.0146>.
- [4] P. Mathivanan, A. Balaji Ganesh, "QR code based color image cryptography for the secured transmission of ECG signal", *Multimedia Tools and Applications*, vol. 78, 6, 2019. <https://doi.org/10.1007/s11042-018-6471-x>.
- [5] J. Rathi, S. K. Grewal, "Aesthetic QR: Approaches for Beautified, Fast Decoding, and Secured QR Codes", *International Journal of Information Engineering and Electronic Business*, Vol. 14, No. 3, 10-18, 2022. <https://doi.org/10.5815/ijieeb.2022.03.02>
- [6] M. M. S. Rani, K.R. Euphrasia, "Data Security Through QR Code Encryption and Steganography", *Advanced Computing: An International Journal*, 7, 1/2, 1-7, 2016. <http://dx.doi.org/10.5121/acij.2016.7201>
- [7] H. N. Abed, "Robust and Secured Image Steganography using LSB and Encryption with QR Code", *Journal of AL-Qadisiyah for computer science and mathematics*, vol. 9, 2, 2017. <https://doi.org/10.29304/jqcm.2017.9.2.144>
- [8] Y. Risqi, R. D. Nyoto, H. Muhandi, "Steganografi QR Code pada Dual Carrier Image dengan Metode Least Significant Bit", *Jurnal Edukasi dan Penelitian Informatika*, vol. 5, 3, 261-271, 2019. <http://dx.doi.org/10.26418/jp.v5i3.35297>
- [9] <https://www.qrcode-tiger.com>
- [10] P. Filzasavitra, T. W. Purboyo and R. E. Saputra, "Analysis of Steganography on PNG hnage using Least Significant Bit (LSB), Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE)", *Journal of Engineering and Applied Sciences*, vol.14, 12, pp. 7821-7827, 2019. <http://dx.doi.org/10.36478/jeasci.2019.7821.78>